**Statement by**
**Amit Yoran**
**Director, National Cyber Security Division, Office of Infrastructure Protection**
**U.S. Department of Homeland Security**

**Before the Subcommittee on Technology**
**Committee on Government Reform**
**U.S. House of Representatives**
**April 21, 2004**

Good morning, Chairman Putnam and distinguished Members of the Subcommittee. My name is Amit Yoran, and I am Director of the National Cyber Security Division the Office of Infrastructure Protection in the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate. I am pleased to appear before you today to discuss DHS' initiatives addressing educational awareness for the cyber citizen focused on protecting our nation's cyberspace. We view awareness as a critical component to our mandate for increasing cyber security and have implemented programs to reach as many people as quickly and effectively as possible. Education and training are critical elements of our strategic initiatives that seek to improve our cyber security posture over the long term and for increasing safety in the cyber world.

## *Introduction*

February 23rd marked the one-year anniversary of the Department of Homeland Security. In his remarks commemorating that day, Secretary Ridge stressed that one of the Department's goals is to strengthen our information sharing capability with respect to securing the nation's critical infrastructure over the next year. We in the Information Analysis and Infrastructure Protection Directorate (IAIP) take that mandate to heart in our collective efforts and activities to protect the Nation. Established by the Homeland Security Act, the IAIP Directorate is the focal point for the Nation to protect our critical infrastructures from attack or disruption. We have made significant strides toward this objective under the leadership of Under Secretary Frank Libutti.

The IAIP Directorate includes the Office of Information Analysis, the primary threat information intelligence gathering and analysis capability of DHS, and the Office of Infrastructure Protection. In today's highly technical and digital world, we recognize that attacks against the nation may manifest themselves in both physical and cyber forms. The interconnected and interdependent nature of our critical infrastructure makes our physical and cyber assets impossible to separate, and it would be irresponsible to address them in isolation. The placement of these two offices within the Directorate underscores this linkage and enables us to work together to share intelligence and other information and coordinate our efforts to mitigate our nation's vulnerabilities. This is why IAIP takes a holistic view of critical infrastructure vulnerabilities and works to protect the nation from all threats by ensuring the integration of physical and cyber security approaches in the Directorate's Office of Infrastructure Protection.

In support of the broader IAIP mission, the National Cyber Security Division (NCSD) was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues. NCSD is charged with coordinating the implementation of the *National Strategy to Secure Cyberspace* released by the President in February 2003.

Under that mandate, DHS works closely with our partners in the federal government, the private sector, and academia on a variety of programs and initiatives to protect our critical infrastructure. We recognize that the challenge is vast and complex, that threats are multi-faceted and global in nature, and that our strengths – and our vulnerabilities – lie in our interdependencies. Further, we acknowledge that the environment changes rapidly and that information sharing and coordination are crucial to improving our overall national and economic security. Cognizant of these realities, DHS' cyber security initiatives and efforts are designed to address each of the priorities set forth in the *National Strategy to Secure Cyberspace* ("the Strategy"):

| | |
|---|---|
| Priority I: | A National Cyberspace Security Response System |
| Priority II: | A National Cyberspace Security Threat and Vulnerability Reduction Program |
| Priority III: | A National Cyberspace Security Awareness and Training Program |
| Priority IV: | Securing Government's Cyberspace |
| Priority V: | National Security and International Cyberspace Security Cooperation |

### ***Cyberspace Security Awareness and Training: A National Priority***

The Strategy recognizes that in addition to vulnerabilities in existing information technology systems, a lack of familiarity, knowledge, and understanding of the issues contribute to the challenge we face in securing our information infrastructure and networks. In its Priority III: A National Cyberspace Security Awareness and Training Program, the Strategy lays out a mandate to address this challenge that calls upon the U.S. Government to promote a comprehensive national awareness program to empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace. Just as we all have an obligation to learn about driving safety rules on the highway for our own personal protection, as well as for the protection of others; we have an equal responsibility to protect ourselves and our Nation by learning about cyber security.

DHS has integrated all of the priorities of the Strategy into our cyber security programs. In addition, we are working closely with other federal agencies, academic institutions, and the private sector toward these objectives.

*Awareness*

The Strategy clearly identifies the users and stakeholders in cyber security in Priority III as home users and small business, large enterprises, institutes of higher education, the private sectors that own and operate the vast majority of the Nation's cyberspace, and state and local governments. We are reaching out to, and partnering with, each of these groups in addition to other groups within the Federal Government.

DHS recognized that in order to meet many of the mandates in the Strategy and other objectives addressing greater national cyber security, we needed to create an operational mechanism for building a cyber security readiness and response system. As such, through an initial partnership with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, we created the U.S. Computer Emergency Readiness Team, or US-CERT. Through the partnership, US-CERT is able to leverage, rather than duplicate, existing capabilities and accelerate national cyber security efforts. US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States, as well as the cyber consequences of physical attacks. To this end, US-CERT is building a cyber watch and warning capability, launching the US-CERT Partnership Program to build situational awareness and cooperation, and coordinating with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber – and physical – attacks. Through its Internet portal, US-CERT is a crucial component of – and a distribution tool for – our cyber security awareness activities.

On January 28, 2004, the Department of Homeland Security, through US-CERT, unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely and actionable information to Americans to secure their computer systems. As the U.S. Government, we have a fundamental duty to warn the public of imminent threats and to provide protective measures when we can, or least provide the information necessary for the public to protect their systems. Furthermore, it is also important to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The offerings of the National Cyber Alert System provide that kind of information, and we have already issued several alerts and the initial products in a periodic series of "best practices" and "how-to" guidance messages. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. I am pleased to report that Americans are exhibiting a keen interest in the alert system. On day one of the National Cyber Alert System launch we had more than one million hits to the US-CERT website. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. As we increase our outreach, the National Cyber Alert System is investigating other vehicles to distribute information to as many Americans as possible. For your reference and for your constituents, I urge you to visit www.us-cert.gov to subscribe to a number of our information services to facilitate protecting your computer systems. We encourage you to include a link to US-CERT on your Committee web page to notify your constituents of the National Cyber Alert System and empower them to sign up to the system to improve their cyber vigilance.

DHS is keenly aware of the power of the media as an education and awareness vehicle. We launched an outreach program concurrent with the launch of the National Cyber Alert System. In nine days, we generated almost one thousand media placements across national newspapers, trade publications, web sites, as well as television and radio broadcast media. Feature coverage on CNN, Fox News, NBC News, National Public Radio, and in *The Wall Street Journal, The Washington Post, Newsweek,* and *The New York Times* generated millions of impressions, increasing American's cyber security awareness and driving citizens to visit the US-CERT website to subscribe to the National Cyber Alert System.

DHS is also a sponsor of the National Cyber Security Alliance (NCSA) and *StaySafeOnline*, a public-private organization created to educate home users and small businesses on cyber security best practices. Other NCSA sponsors include: The Federal Trade Commission, AT&T, America Online, Computer Associates, ITAA, Network Associates, and Symantec. DHS is providing matching funds to expand the NCSA end-user outreach campaign, which will include a Fall 2004 Public Service Announcement to increase awareness among Americans about key cyber security issues. We look forward to working actively with the NCSA to increase the profile and impact of its semi-annual National Cyber Security Day initiative. Coincident with the days that we reset our clocks in the spring and fall, the National Cyber Security Day program encourages Americans to review and improve their cyber readiness. We will utilize the National Cyber Security Days as a focal point to heighten our awareness efforts. We encourage each of you to take advantage of this program to hold a cyber security event in your respective districts in conjunction with the next National Cyber Security Day – October 31. In addition, we are working with NCSA on a series of other educational and awareness programs, including collaborative initiatives with Internet Service Providers and developing cyber security educational tool kits. We will be pleased to make these resources available to you for use in your districts.

The Federal Trade Commission (FTC) has also been very active in building awareness with home users and small businesses, and I am pleased that Commissioner Swindle is here to share the FTC's initiatives with you. As referenced earlier, the FTC plays a significant role in NCSA. The Commissioner has been a leading force in the FTC's information security campaign, and we work closely with his team.

It is estimated that 85 percent of America's critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003, the National Cyber Security Division co-hosted the first National Cyber Security Summit in Santa Clara, California, with the Information Technology Association of America, TechNet, the Business Software Alliance, and the U.S. Chamber of Commerce. This event was designed to energize the public and private sectors to implement the *National Strategy to Secure Cyberspace*. The Summit allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber security issues facing the Nation. Five industry task forces were established to focus specifically in the areas of:

- Increasing awareness
- Cyber security early warning
- Best practices for information security corporate governance
- Technical standards and common criteria
- Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from developing a national strategy to energizing the public-private partnership to implement concrete, measurable actions to improve the security of America's cyber systems. Over the past few weeks, the industry task forces have put forward sets of recommendations in each of these key areas for both the public and private sector. DHS is reviewing these recommendations, as well as those put forth by other industry and government groups. We are excited that the industry is showing such initiative.

DHS is establishing the US-CERT Partnership Program as our primary mechanism for responding to these various recommendations. As previously indicated, collaboration between the public and private sectors is crucial to achieving greater cyber security, as both have specific and important roles to play. We are developing the components of the US-CERT Partnership Program based on recommendations of the task forces, the National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC), your own committee's working groups, and other similar groups. The goal of the partnership is to facilitate and leverage stakeholder collaboration to drive measurable progress in addressing key cyber security issues and mitigating our cyber vulnerabilities. DHS is moving with great urgency to put this partnership into place. We are working closely with the private and public sectors to implement an effective program.

Under the auspices of the US-CERT Partnership Program, DHS will work jointly with software developers, academic institutions, researchers, and communities of interest including the Information Sharing and Analysis Centers (ISACs) in each of the critical infrastructure sectors outlined in Homeland Security Presidential Directive 7 (HSPD 7) as well as with our federal, state, local, and international government counterparts. Our goal is to participate in, coordinate, and help refine current activities and define future programs that will improve our national cyber security. We are already working closely with many of these organizations, such as the Multi-State ISAC and the National Association of State Chief Information Officers (NASCIO), to shape the program and to understand hurdles in our path forward.

*Training and Education*

In addition to awareness, I would highlight another key aspect of the Strategy's Priority III: training and education. The Strategy specifically calls for efforts to foster adequate training and education programs to support the Nation's cyber security needs and increase the efficiency of existing federal cyber security training programs.

DHS is collaborating with our intergovernmental partners to leverage and build upon their ongoing training and education programs, and we are also reaching out to academic institutions to establish cooperative arrangements. I would like to highlight two recent accomplishments in this regard.

First, I am pleased to announce that DHS has just signed on to partner with the NSA to expand its program from an NSA-specific focus to a broader national program. To reflect the expanded scope, the program is renamed, the new *National* Centers of Academic Excellence in Information Assurance Education Program.

The traditional Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program was established by the NSA in 1998 to promote higher education in information assurance, and as such, increase the number of information security professionals with this critical expertise. NSA grants the CAEIAE designation following a rigorous review of university applications against published criteria based on training standards established by the National Security Telecommunications and Information Systems Security Committee, an intergovernmental organization that sets policy for the security of national security systems. The criteria measure the depth and maturity of established programs in the field of information assurance. Since its inception, the program has been highly successful, designating 50 universities in 26 states.[1] Universities designated as Centers are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs.

The new, increased scope will accelerate and expand the current program, help attain national prominence, and attract participation from other universities. The net result is that America will be furnished with a growing number of cyber security professionals. Government at all levels; corporations, small businesses, and the general public all benefit from educating a strong force of highly educated information assurance professionals.

Second, I am pleased to announce that DHS has partnered with the National Science Foundation on the Scholarship for Service program. This initiative promotes

[1] See Appendix for list of CAEIAE-designated universities.

university level information assurance education and efficiently places program graduates into the federal workforce.

NSF established the Scholarship for Service Program in 2001 to train a corps of information assurance (IA) specialists and place them in federal agencies for the protection of the U.S. Government's information infrastructure. The program provides two-year scholarships to graduate and upper-level undergraduate students and, in return, those students are required to make a commitment to work for a federal civilian agency for two years. NSF projects that 81 students will graduate in May 2004, and our goal is to graduate 300 students into the program annually. The qualifications of the program graduates are outstanding. DHS, as well as US-CERT, have already hired several graduates. We are excited about the capabilities this program is producing.

In addition to these accomplishments, we have identified other strategic education programs. We are working with the Department of Education to develop cyber security programs for the K-12 curriculum in our public schools. These children are our future, and they are working on computers at a very young age. It is important to educate and raise them in a secure cyber culture from the beginning.

## Conclusion

DHS views building awareness as a key, immediate, and daily objective for addressing our national cyber security. We have operationalized that function through US-CERT, the National Cyber Alert System, and our partnerships with industry, academia, and others. In addition, we know we have an obligation to address cyber security in more strategic way for the long term, and we are targeting our education and training programs to work to ensure that we have a cadre of trained security professionals to carry on that task as technology continues to evolve and change our lives over time. We have made some important strides in both these operational and strategic efforts, and we are committed to improving and expanding on them going forward.

In closing, I would add one important additional strategic systemic consideration – we need to change the DNA of technology offerings to make it easier for people to understand and deploy cyber security. While I commend the technology solution provider community for its major steps forward in auto-updating and auto-configuration management, and the like, there is much work ahead. The technology community at large needs to redouble our collective efforts to produce secure code that is easier to maintain and manage. The US-CERT Partnership Program brings together solution providers, critical infrastructure operations, educational institutions, and end-user advocacy groups to tackle these systemic issues. Our goal is to ensure that all computer users understand the rules of the road for cyber security and are empowered to stay safe online.

Thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.

# APPENDIX

## Centers of Academic Excellence in Information Assurance Education (CAEIAE)

### Alabama

Auburn University

### California

Naval Postgraduate School

Stanford University

University of California at Davis

### Florida

Florida State University

### Georgia

Georgia Institute of Technology

### Idaho

Idaho State University

University of Idaho

### Illinois

University of Illinois at Urbana-Champaign

### Indiana

Purdue University

## Iowa

Iowa State University

## Maryland

Capital College

Johns Hopkins University

Towson University

University of Maryland, Baltimore County

University of Maryland, University College

## Massachusetts

Northeastern University

University of Massachusetts, Amherst

## Michigan

Walsh College

## Mississippi

Mississippi State University

## Nebraska

University of Nebraska at Omaha

## New Jersey

New Jersey Institute of Technology

Stevens Institute of Technology

## New Mexico

New Mexico Tech

## New York

Pace University

Polytechnic

State University of New York, Buffalo

State University of New York, Stony Brook

Syracuse University

U.S. Military Academy, West Point

## North Carolina

North Carolina State University

University of North Carolina, Charlotte

## Ohio

Air Force Institute of Technology

## Oklahoma

University of Tulsa

## Oregon

Portland State University

## Pennsylvania

Carnegie Mellon University

Drexel University

East Stroudsburg University

Indiana University of Pennsylvania

Pennsylvania State University

University of Pennsylvania

**Texas**

Texas A&M University

University of Dallas

University of Texas, San Antonio

**Vermont**

Norwich University

**Virginia**

George Mason University

James Madison University

University of Virginia

**Washington, D.C.**

George Washington University

Information Resources Management College

**West Virginia**

West Virginia University